Sumário

Primeiros passos...

Prezado(a) usuário(a)!

Agradecemos que você tenha optado por um produto G Data e esperamos que esteja sempre satisfeito com seu novo software. Caso algo não funcione imediatamente, talvez a nossa documentação da ajuda possa ajudá-lo(a). Para perguntas, críticas e sugestões, a nossa equipe de especialistas no **G Data Suporte técnico** está disponível.

Esta introdução ajuda a instalar seu novo software G Data e fornece algumas dicas práticas para utilização.

Você tem mais alguma dúvida? No software, é possível abrir a qualquer momento a ajuda detalhada do programa. Para isso, basta pressionar no programa a tecla **F1** ou clicar no botão da Ajuda aqui ilustrado.

Suporte técnico

A instalação e utilização do software G Data são intuitivas e descomplicadas. Caso ocorra algum problema, simplesmente entre em contato com os funcionários especializados do nosso Suporte técnico:

www.gdatasoftware.com.br

Instalação

Para o funcionamento correto do software, o seu computador deve atender aos seguintes **requisitos mínimos** dependendo do sistema operacional:

- Microsoft Windows 7 / Vista (32/64bit), memória de trabalho disponível de 1 GB,
- Microsoft Windows XP (SP2 ou superior, 32bit), memória de trabalho disponível de 512 MB.

Se o seu computador for novo de fábrica ou tiver sido protegido até agora por um software antivírus, será possível executar a instalação com as etapas a seguir. Mas, se você tiver a suspeita fundada que o seu computador está infectado com vírus, recomenda-se a realização de um **BootScan** antes da instalação do software G Data. Para isto, leia o capítulo **BootScan**.

Etapa 1

Além da instalação clássica de software com CDs ou DVDs, agora há outras possibilidades da instalação de software:

- **Instalação com CD/DVD**: Para começar a instalação, insira o CD ou DVD do software G Data. Uma janela de instalação é aberta automaticamente.
- **Instalação do pen drive USB**: Caso você tenha comprado o software em um pen drive USB, conecte o pen drive USB com o seu computador. Uma janela de instalação é aberta automaticamente.
- **Download do software**: Para começar com a instalação de uma versão do software baixada da internet, faça simplesmente um clique duplo no arquivo baixado. Uma janela de instalação é aberta automaticamente.

Etapa 2

Agora, clique no botão **Instalar**. Agora, um assistente o ajudará com a instalação do Software no seu computador.

Etapa 3

Durante a instalação, acontece a **ativação do produto**. Aqui você pode ativar o seu software.

- **Inserir o número de registro**: Ao instalar o seu software G Data pela primeira vez, selecione esta opção e, a seguir, insira o número de registro que acompanha o produto. Dependendo do tipo do produto, o número pode ser encontrado, por exemplo, no verso do manual de instruções, no e-mail de confirmação do download do software ou na capa do CD.

    Ao inserir o número de registro, o seu produto será ativado e, além disso, você receberá um e-mail com os dados de acesso para a futura utilização.

    Se tiver problemas na inserção do número de registro, verifique o Número de registro. Dependendo do tipo de letras utilizado, muitas vezes interpreta-se um "I" maiúsculo (como Ida) erroneamente como o número "1" ou a letra "l" (como Ludwig). O mesmo vale para: "B" e "8", "G" e 6, "O" e "0", "Z" e "2".

- **Inserir dados de acesso**: Se você já ativou o seu software G Data anteriormente, então você recebeu seus dados de acesso (**nome de usuário** e **senha**). Para instalar o software G Data novamente ou para registrar mais computadores com uma licença multiusuário, simplesmente insira os seus dados de acesso aqui.

    Você recebe os dados de acesso exclusivamente por e-mail. Os dados de acesso não estão acompanhando o produto.

    Se tiver perdido ou esquecido os seus dados de acesso, clique, para se conectar, no registro **Perdeu os seus dados de acesso?** Uma página será aberta onde será possível inserir novamente o número de registro. Após inseri-los, os dados de acesso serão enviados ao endereço do e-mail informado no registro. Se o seu **endereço de e-mail** mudou nesse período, entre em contato com a nosso **Suporte técnico**.

- **Versão de teste**: Para conhecer o softwareG Data gratuitamente, você pode utilizar simplesmente o nosso acesso de teste temporário. Informe aqui um endereço de e-mail válido e o seu nome e você receberá de nós os dados de acesso via e-mail.

- **Ativar mais tarde**: Se você quiser simplesmente dar uma olhada no software, você pode instalá-lo também sem a informação de dados. Mas, desta forma o programa não descarrega atualizações da internet e, portanto, não haverá uma proteção real contra software malicioso. Você pode informar o número de registro ou os seus dados de acesso a qualquer tempo posteriormente, assim que você executar uma atualização.

O software G Data pode proteger o seu computador eficientemente apenas com atualizações atuais do dia. A utilização do software sem a ativação protege você apenas insuficientemente.

Etapa 4

Talvez você precise reiniciar o seu computador após a instalação. Então, o software G Data estará à sua disposição.

Caso a instalação não inicialize: Pode ser que a **função inicialização automática** de seu computador não esteja configurada corretamente. Então, o software não pode iniciar o procedimento da instalação após a introdução do CD de programa (ou a conexão do pen drive USB na versão do pen drive USB do software G Data) e não é aberta nenhuma janela com qual você possa instalar o software G Data.

- Se, ao invés disso, uma janela de opções for aberta para uma reprodução automática, clique na opção **Executar AUTOSTRT. EXE**.
- e uma janela de seleção não for aberta, procure no seu Windows Explorer a mídia de dados com software G Data e então inicie o arquivo **Setup** ou, conforme o caso, **Setup.exe.**

Assim, aparecerá a janela de instalação de seu software G Data e você pode iniciar a instalação.

Após a instalação

Para abrir a interface de programa do seu software, simplesmente clique duas vezes no **ícone da área de trabalho** ilustrado aqui. Para saber como utilizar a SecurityCenter. leio o capítulo: **SecurityCenter**.

G Data Ícone: Seu software G Data protege seu computador permanentemente contra softwares maliciosos e ataques. Um ícone G Data na barra de tarefas do seu computador alerta você assim que o software determina a necessidade de uma intervenção do usuário. Informações avançadas podem ser obtidas no capítulo: **Para que serve o ícone G Data?**

Verificação rápida: Com a verificação rápida, você pode verificar arquivos de forma simples, mesmo sem precisar iniciar o software. Basta marcar com o mouse os arquivos ou a pasta, por exemplo, no Windows Explorer. Clique então no botão direito do mouse e selecione na janela de diálogo que surge **Verificar a existência de vírus**. Uma verificação automática dos respectivos arquivos será executada.

G Data Triturador: Caso você tenha selecionado o triturador na instalação, este poderá ser acessado por meio do ícone na área de trabalho. Dados jogados no triturador são eliminados de forma que não podem mais ser restaurados, mesmo com ferramentas profissionais de recuperação de dados. Alternativamente, você pode clicar um arquivo com o botão direito do mouse e selecionar **Triturar**. O triturador não está disponível na versão de programa **G DataAntiVirus**.

Após a instalação do softwareG Data **, seu computador inicia diferentemente do habitual**: Se, após a instalação do software G Data, o computador não iniciar diretamente com o Microsoft Windows em uma próxima reinicialização, pode ser em razão de o CD G Data ainda se encontrar dentro da unidade de CD. Ele serve ao mesmo tempo como CD de boot que pode iniciar antes do sistema operacional para executar um BootScan, caso necessário. Simplesmente remova o CD e reinicie o computador da maneira habitual. Informações avançadas podem ser obtidas no capítulo: **BootScan**

SecurityCenter

Após a instalação, a sua proteção antiVirus, em princípio, é executada de forma totalmente automática. A SecurityCenter precisa ser chamada somente quando você desejar acessar uma das muitas funções adicionais do software. Em todos os casos em que o software exija sua intervenção, você será automaticamente lembrado sobre as informações na barra de tarefas do computador.

Com um clique, é possível eliminar do caminho as possíveis ameaças ao seu computador. Para isso, está disponível o símbolo do **Status da proteção**.

Enquanto uma marcação verde estiver acesa ao lado do registro **Segurança** o seu sistema estará protegido.

Um ponto de exclamação vermelho indica que há um perigo iminente para o seu sistema. Você deverá tomar providências imediatas para que seus dados permaneçam protegidos.

Quando você clica no botão **Corrigir**, o software sugere as ações que devem ser executadas para continuar protegendo o seu sistema de forma ideal. Selecione as ações exibidas uma após a outra, até que o status da proteção mostre novamente uma luz verde. O botão muda automaticamente para inativo e só poderá ser utilizado novamente se o status da proteção piorar. Assim o seu software estará novamente no estado mais recente e você poderá fechar novamente a SecurityCenter. Além disso, existem ainda as seguintes mensagens de status:

Um símbolo amarelo indica que é necessária uma intervenção rápida pelo usuário.

Se o símbolo de espaço reservado for exibido, significa que você não ativou a respectiva função de segurança (por ex., proteção contra spam).

Todas as funções e configurações vistas abaixo do símbolo do status da proteção (como **proteção antiVirus** ou **assinaturas de vírus**) podem ser utilizadas quando você desejar se ocupar ativamente da segurança do seu sistema, mas isso não é necessário! Decida você mesmo como deseja se ocupar do assunto da Proteção antivírus. Nas respectivas subseções, você vê detalhadamente as áreas que o seu software ajustou de forma ideal e quais poderão ser melhoradas. Os ícones a seguir indicam o status de segurança da respectiva área.

Configurações: Através desse botão na parte superior direita, você pode acessar todos os diálogos de configuração das diversas áreas do software. Na respectiva área, você também tem a possibilidade de selecionar diretamente o diálogo de configuração adequado.

Para isso, se necessário, leia também o capítulo: **Configurações**

Além disso, à direita, ao lado do símbolo de configuração, podem ser encontradas as seguintes funções adicionais:

Exibir ajuda: No software, é possível abrir a qualquer momento a ajuda detalhada do programa. Para isso, basta pressionar no programa a tecla F1 ou clicar no botão de Ajuda aqui ilustrado.

Registros: O software lista aqui os registros atuais relativos a todas as funções executadas (verificação de vírus, atualização, detecção de vírus etc.).

Criar CD de boot: O BootCD é uma ferramenta útil para tornar computadores já infectados, livres de vírus. Principalmente para computadores que, antes da instalação do software G Data não tinham nenhuma proteção antiVirus, recomenda-se a utilização de um BootCD. As informações sobre como criar e utilizar um **CD de boot** podem ser lidas no capítulo: **BootScan antes da instalação**.

As funções descritas, como por exemplo, a criação de um CD de boot não estão disponibilizadas? Pode ser que a opção **Criar CD de boot** não tenha sido instalada com o software G Data. Esta pode ser facilmente instalada posteriormente, inserindo novamente o CD do software e executando a instalação com a opção BootCD.

Atualizar programa: Quando existirem novas versões do programa do software, você poderá atualizá-las, bem como as informações de vírus, de forma confortável através de cliques. Se obtiver a informação de que uma atualização na Internet está disponível, basta clicar no registro **Atualizar programa**.

Problemas com a atualização na Internet? Informações detalhadas podem ser obtidas no capítulo: **Atualizações**

Informações: Aqui você obtém informações sobre a **versão do programa**. O número da versão pode, por exemplo, ser útil para o contato com o **Suporte técnico**.

Licença

Abaixo do registro **Licença**, no lado esquerdo da interface do programa, você verá por quanto tempo a licença para atualizações de vírus ainda será válida. Em nenhum outro software, as atualizações constantes são tão importantes quanto nos softwares antivírus. Antes que a sua licença expire, o software lembra você automaticamente para renovar a sua licença. A forma mais confortável e descomplicada de fazer isso é pela internet.

O que acontece quando a minha licença expira?

Alguns dias antes de sua licença expirar, aparece uma janela de informações na barra de tarefas. Clicando, abre-se uma caixa de diálogo na qual você pode prorrogar a sua licença sem problemas diretamente, em poucos passos. Clique simplesmente no botão **Comprar agora**, complete os seus dados e a proteção antiVirus está novamente garantida imediatamente. Você receberá a fatura confortavelmente nos próximos dias via correio.

Esta caixa de diálogo aparece apenas após o término do primeiro ano. Depois disso, a sua licença G Data é prorrogada automaticamente a cada ano. Mas você pode cancelar essa assinatura a qualquer hora e sem mencionar as razões.

Como posso receber licenças adicionais/estendidas?

Naturalmente é possível ampliar o número de suas licenças ou fazer uma atualização dos produtos com um maior volume de funções. Se clicar no registro **Estender licenças**, na SecurityCenter, será direcionado para o site de nossa loja online.

Carga na CPU

Sob o título **G Data**, você vê a carga atual ocupada pelo software em seu computador. Abaixo, sob a legenda **Sistema** - você vê a utilização total atual do seu computador. Durante as verificações, a utilização do sistema pelo software G Datapode ser altíssima, mas, durante a operação normal da sentinela, o software G Data utiliza muito pouco a capacidade do processador. Portanto, se o seu computador reagir de forma mais lenta do que a habitual, aqui você poderá detectar rapidamente se o software G Data está momentaneamente executando uma verificação intensiva ou se o computador está sendo restringido por um outro motivo que não esteja relacionado à verificação do sistema.

Além disso, o software G Data está instalado de forma que o seu computador só faz a verificação se não estiver sendo utilizado. Como um protetor de tela, a verificação de vírus ocorre sempre só quando você não é perturbado. Naturalmente a proteção antiVirus permanente através da sentinela de vírus está completamente ativa o tempo todo.

- **Verificação de vírus**: A verificação regular, se não há vírus ou programas maliciosos aninhados no seu computador.
- **Sentinela de vírus**: A proteção geral do seu computador contra software malicioso invasor.

Proteção AntiVirus

Nesta área, você recebe informações sobre quando foi a última vez que o seu computador foi verificado por vírus e se a sentinela de vírus o protege ativamente contra infecções no momento.

Última verificação de vírus

Aqui é exibido quando o computador foi totalmente controlado pela última vez, quanto à infecção por vírus. Quando esse registro estiver marcado em vermelho, você deverá executar o mais rápido possível uma verificação de vírus. Para isto, basta clicar no registro e poderá iniciar o processo de verificação, clicando no botão **Verificar computador**. Após a verificação, o registro estará marcado em verde, uma indicação que uma verificação de vírus foi feita em um período suficiente.

Para saber como é o processo de uma verificação de vírus e o que deverá ser feito se realmente um vírus for encontrado, leia o capítulo: **O que ocorre em uma verificação de vírus?**

Sentinela de vírus

A Sentinela de vírus deve sempre estar ativa. Se desejar desativar a sentinela em algum momento ou desejar efetuar alterações nas configurações, clique no registro **Desativar sentinela de vírus**.

Verificação de vírus e sentinela de vírus: Ambas as funções servem para proteger o seu computador contra infecções, mas têm uma abordagem diferente.

- A **Sentinela de vírus** verifica continuamente o seu computador quanto à existência de vírus e controla os processos de gravação e leitura; assim que um programa desejar executar funções maliciosas ou propagar arquivos danosos, a sentinela de vírus o impede. A Sentinela de vírus é uma proteção importante! Ela não deve nunca ser desativada.

- A **Verificação de vírus** é uma proteção adicional. Ela verifica se um vírus não se encontra no seu sistema. Uma verificação de vírus encontraria mesmo os vírus que foram copiados para o seu computador antes da instalação do software G Data ou que você tenha recebido com a Sentinela de vírus desativada. Uma verificação de vírus deve ser feita em intervalos regulares, preferencialmente em períodos automáticos, durante os quais o seu computador não for necessário.

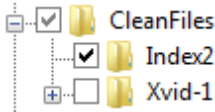
Menu de seleção

Clicando diretamente no título **Proteção antiVirus**, aparecerá uma seleção de ações que podem ser efetuadas diretamente aqui.

Verificar computador: Quando desejar controlar o seu computador de forma independente da verificação automática (p. ex., devido a uma suspeita de vírus), bastará clicar neste registro. O seu computador será diretamente verificado quanto a infecções por vírus. Para isso, leia também o capítulo **O que ocorre em uma verificação de vírus**.

Verificar memória e inicialização automática: Através desta opção, para todos os Processos em andamento são verificados os arquivos de programa e as bibliotecas de programas (DLLs). Dessa forma, os programas maliciosos poderão ser removidos diretamente da **Memória** e da **Área de inicialização automática**. Vírus ativos podem ser removidos diretamente, sem que o disco rígido tenha que ser totalmente pesquisado. Como essa verificação pode ser executada relativamente rápida, é recomendável fazê-la constantemente no escopo de uma verificação de vírus automática. Essa função não é uma substituição de um controle de vírus constante dos dados armazenados, ela é apenas uma complementação.

Verificar diretórios/arquivos: Através dessa opção, você verifica a existência de vírus em unidades, diretórios ou arquivos. Ao clicar nesta ação, uma opção de diretório e arquivo é aberta. Aqui é possível verificar objetivamente a existência de infecção de vírus em arquivos individuais e também em diretórios completos.

Na árvore de diretórios (à esquerda), clicando nos sinais (+), é possível abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo. Cada diretório ou arquivo com uma marcação será verificado pelo software. Se nem todos os arquivos tiverem que ser verificados em um diretório, haverá uma marcação em cinza nesse diretório.

Verificar mídias removíveis: Com esta função, verifique **CD-ROMs** ou **DVD-ROMs**, **cartões de memória** ou **pen drives** quanto à infecção por vírus. Ao clicar nessa ação, todas as Mídias removíveis que estiverem conectadas ao seu computador (ou seja, também CDs inseridos, cartões de memória ou Discos rígidos conectados por USB ou Pen drives) serão verificadas. Observe que o software não poderá naturalmente remover vírus de mídias que não permitam acesso à gravação (p.ex., CD-ROMs gravados). Uma eventual detecção de vírus será registrada.

Verificar a existência de Rootkits: Os **Rootkits** tentam escapar dos métodos comuns de detecção de vírus. Com essa função, é possível procurar por rootkits de forma objetiva, sem ter de executar uma verificação completa dos discos rígidos e dados armazenados.

Desativar verificação em modo ocioso: Enquanto a sentinela de vírus protege o seu sistema permanentemente contra software malicioso, a **verificação em modo ocioso** é uma verificação inteligente de vírus que verifica todos os arquivos do seu computador continuamente por infecções de vírus. A verificação em modo ocioso trabalha como uma proteção de tela, apenas quando você não necessita do seu computador por um tempo. Assim que você continuar a trabalhar, ela para e garante o desempenho ideal para o trabalho.

Naturalmente, o seu computador continua protegido pela sentinela de vírus, mesmo se a verificação em modo ocioso for desativada. Isso pode ser útil se você, por exemplo, preferir iniciar uma verificação de vírus do sistema manualmente.

Desativar sentinela de vírus: Com esta opção, é possível desativar a **Sentinela de vírus**, em caso de necessidade, e também ativá-la novamente. Isso pode ser útil, p.ex, quando uma grande quantidade de dados em seu disco rígido é copiada de um local para outro ou para rodar processos de exibição que ocupam muito espaço na memória (copiar DVDs e outros). Você deverá desativar a sentinela de vírus apenas pelo período necessário. Deve-se ter a certeza de que o sistema durante esse período, se possível, não esteja conectado à Internet ou possa acessar dados novos e não verificados (p.ex, através de CDs, DVDs, placas de memória ou dispositivos USB).

Quarentena: A quarentena é uma área protegida dentro dentro do software onde os arquivos infectados são armazenados de forma codificada e, dessa forma, o vírus não pode mais ser repassado a outros arquivos. Leia para isso também o capítulo: **Como funciona a quarentena?**

Configurações:Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - AntiVirus**

Assinaturas de virus

Nesta área, você recebe informações sobre as últimas atualizações do programa.

Última atualização

Aqui se visualiza quando foi a última vez que o seu computador recebeu as atuais assinaturas de vírus da internet. Quando esse registro estiver marcado em vermelho, você deverá executar o mais rápido possível uma atualização de vírus. Clique simplesmente no registro e selecione a opção **Atualizar assinaturas de vírus**.

Próxima atualização

Nesse registro é possível visualizar a próxima atualização prevista.

> **Assinaturas de vírus**: Vírus e outros programas maliciosos podem ser reconhecidos por atributos característicos. Seu software G Data possui funções que detectam os vírus também pelo seu comportamento. A detecção e o combate ao respectivo programa malicioso ficam incomparavelmente mais rápidos e mais eficientes com uma assinatura de vírus, comparável com um mandado de captura. A proteção antiVirus ficará realmente segura apenas com a atualização regular desses mandados de captura dos bancos de dados G Data na internet.

Menu de seleção

Clicando diretamente no título **Assinaturas de vírus**, aparece uma seleção de ações que podem ser efetuadas diretamente aqui.

Atualizar assinaturas de vírus: Normalmente, as atualizações das assinaturas de vírus são efetuadas de forma automática. Caso queira efetuar uma atualização imediatamente, clique neste botão.

Desativar atualizações automáticas: Caso que você não queira que o software G Data cuide da atualização das assinaturas de vírus automaticamente, você pode selecionar esta opção. No entanto, a desativação significa um alto risco de segurança e deve ser efetuada apenas em casos excepcionais.

Configurações: Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - AntiVirus**

Proteção da web

Nesta área você pode ativar ou desativar a proteção da web. A proteção da web é um módulo que reconhece e, eventualmente, elimina automaticamente ameaças durante a navegação na internet ou durante downloads. Ela serve como apoio adequado da sentinela de vírus e bloqueia websites maliciosos e downloads já antes de serem acessados.

Se uma página da internet for reconhecida como ameaça pelo software G Data, você receberá, em vez da website, uma página de informações da G Data no navegador.

Menu de seleção

Clicando diretamente no título **Proteção da web**, aparecerá uma seleção de ações que podem ser efetuadas diretamente aqui.

Definir exceções: A proteção da web cuida para que você não seja vítima de sites infectados ou fraudulentos. Em alguns raros casos, pode ocorrer que uma página da Internet não seja corretamente exibida, apesar de originar de um ofertante seguro. Nesses casos, você pode colocar os endereços da Internet na Whitelist, ou seja você pode defini-la, como exceção e a proteção da web não a bloqueará mais. Leia no capítulo **Definir exceções** como isso é feito.

Whitelist: Uma seleção de objetos (p.ex. páginas da internet) que são considerados inofensivos pelo usuário e que não são verificados especialmente.

Desativar Proteção da web: A desativação da Proteção da web pode proporcionar, p.ex., uma vantagem de tempo em grandes downloads de fonte segura. A princípio, o seu computador é protegido pela sentinela de vírus, mesmo sem proteção da web. Entretanto, você deverá abrir mão da proteção da web apenas em casos excepcionais.

Configurações: Com este botão, você pode acessar opções de configuração básicas, se for necessário. Para isso, leia o capítulo: **Configurações - Proteção da web**

Configurações

Na área **Configurações**, você pode configurar os respectivos módulos dos programas de acordo com as suas preferências. Via de regra, não é necessário executar aqui as alterações, pois o software G Data já foi configurado de maneira ideal para o seu sistema na instalação.

AntiVirus

Aqui você encontra todas as possibilidades de configuração sobre o tema proteção antiVirus.

Sentinela

Na caixa de diálogo **Opções** da **Sentinela de vírus**, você tem as seguintes opções de configuração. Somente em casos especiais, é necessário fazer alterações aqui:

- **Status da sentinela**: Aqui você determina se a sentinela deve ser ativada ou desativada.
- **Utilizar mecanismos**: O software trabalha com dois **mecanismos** (engine = máquina/motor em inglês), ou seja, dois programas de verificação de vírus independentes entre si. Cada mecanismo, por si só, já protegeria contra vírus, em alta escala, mas, exatamente a combinação de ambos os mecanismos, oferece os melhores resultados. Em computadores antigos e lentos, é possível, mediante a utilização de apenas um único mecanismo, acelerar a verificação de vírus; no entanto, via de regra, deve-se manter a configuração **Ambos os mecanismos**.
- **Arquivos infectados**: Ao detectar um vírus, a configuração padrão pergunta o que você deseja fazer com o vírus e o arquivo infectado. Quando desejar executar sempre a mesma ação, poderá definir isto aqui. A máxima segurança para os seus dados é oferecida pela configuração **Desinfectar (se não for possível: para quarentena) quarentena))**.
- **Pastas infectadas**: Defina aqui se as **pastas** (por exemplo, arquivos com a extensão **RAR**, **ZIP** ou também **PST**) deverão ser tratados de forma diferente dos arquivos normais. No entanto, observe que mover um arquivo compactado para a quarentena pode danificá-lo, de forma que ele também não poderá mais ser usado após movê-lo de volta. Por essa razão, em caso de pastas infectadas, recomenda-se decidir caso a caso e selecionar **Perguntar as ações desejadas**.

- **Proteção do sistema**: Se o monitoramento do comportamento for ativado, toda a atividade no sistema será monitorada independentemente da sentinela de vírus. Assim, identificam-se também pragas que ainda não possuem uma assinatura. O monitoramento do comportamento protege especialmente contra modificações na inicialização automática e no arquivo host.

Exceções

Clicando no botão **Exceções** você pode excluir determinadas unidades, diretórios ou arquivos da verificação e, dessa forma, acelerar significativamente o reconhecimento de vírus. Para isso, proceda da seguinte forma:

1. Clique no botão **Exceções**.

2. Na janela **Exceções da sentinela**, clique em **Nova**.

3. Selecione agora se deseja que a exceção seja aplicada a uma unidade de disco, um diretório, arquivo ou tipo de arquivo.

4. Então, selecione abaixo o diretório ou a unidade que deseja proteger. Para proteger arquivos, digite o nome completo do arquivo no campo de entrada na máscara de arquivos. Aqui também é possível trabalhar com **Espaços reservados**.

   A forma de funcionamento dos Espaços reservados é a seguinte:

   - O **ponto de interrogação** (?) é substituto para caracteres individuais.
   - * O **asterisco** (*) é substituto para seqüências de caracteres inteiras.

   Para, por exemplo, proteger todos os arquivos com a extensão **.sav** , digite ***.sav**. Para proteger uma seleção especial com nomes de arquivo sequenciais, (p.ex., text1.doc, text2,doc, text3.doc), digite, por exemplo, **text?.doc**.

Esse processo pode ser repetido quantas vezes desejar e também, é possível excluir ou modificar novamente as exceções existentes.

Avançado

Defina com um clique no botão **Avançado** que verificações adicionais deverão ser executadas pela Sentinela de vírus. Normalmente, nenhuma outra configuração é necessária aqui.

- **Modo**: Aqui você pode determinar se os arquivos na execução devem ser verificados apenas na leitura ou na escrita e na leitura. Se a verificação acontecer na escrita de um arquivo, verifica-se diretamente na criação de um novo arquivo ou uma versão do arquivo se este arquivo eventualmente foi infectado por um processo desconhecido. Caso contrário, os arquivos serão verificados apenas quando lidos por programas.
- **Verificar acessos à rede**: Se houver uma conexão de rede do seu computador para computadores desprotegidos (p.ex., Notebooks de terceiros), é recomendável verificar também a existência da transferência de programas maliciosos no acesso à rede. Se utilizar o seu computador de forma individual sem acesso à rede, essa opção não precisa ser ativada. Se tiver instalado uma proteção antivírus em todos os computadores da rede, recomenda-se também, desativar essa opção, porque alguns dados poderão ser verificados duplamente, o que causará um efeito negativo na velocidade.
- **Heurística**: Na análise heurística, os vírus não são reconhecidos apenas por meio da atualização de vírus, obtida regularmente online, mas, com base em determinadas características típicas de vírus. Esse método é mais uma vantagem de segurança, no entanto, em raros casos, pode levar a um alarme falso.
- **Verificar pastas (compactadas)**: A verificação de dados em arquivos compactados (reconhecidos através das extensões de arquivo **ZIP**, **RAR** ou também **PST**) demanda muito tempo e normalmente pode ser ignorada quando a Sentinela de vírus estiver, em geral, ativada no sistema. Para aumentar a velocidade da verificação de vírus, você pode limitar o tamanho das pastas, que serão verificadas, para um determinado valor em megabytes.
- **Verificar pastas de e-mail**: Como o software já verifica a infecção de vírus na entrada e na saída de e-mails, na maioria dos casos, é recomendável não fazer a verificação regular da pasta de e-mail, porque esse procedimento, dependendo do tamanho da pasta, poderá demorar alguns minutos.

- **Verificar áreas do sistema na inicialização do sistema**: As áreas de sistema (p.ex., setores de boot) do seu computador não devem ser ignoradas no controle de vírus. Aqui você pode definir se essas áreas devem ser verificadas na **inicialização do sistema** ou na **troca de mídia (por ex., novo** CD-ROM). Normalmente, pelo menos uma dessas duas funções deve estar ativada.
- **Verificar áreas de sistema na troca de mídia**: As áreas de sistema (p. ex., setores de boot) do seu computador não devem ser ignoradas no controle de vírus. Aqui você pode definir se essas áreas devem ser verificadas na inicialização do sistema ou na **troca de mídia** (p.ex., novo CD-ROM). Normalmente, pelo menos uma dessas duas funções deve estar ativada.
- **Verificar Discador/Spyware/Adware/Riskware**: Com este software, o seu sistema pode ser verificado também quanto a **Discadores** e outros programas maliciosos (**spyware**, **adware** e **riskware**). Aqui, trata-se de programas que estabelecem caras e indesejadas conexões à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, que p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.
- **Verificar somente arquivos novos ou alterados**: Se você ativar esta função, serão verificados somente os arquivos que não são alterados há muito tempo e que antes tinham sido reconhecidos como inofensivos. Isso leva a um ganho de desempenho no trabalho diário – sem risco de segurança.

Verificação manual de vírus

Aqui é possível efetuar configurações básicas do programa para a **Verificação de vírus**. No entanto, isso não é necessário para o funcionamento normal.

- **Utilizar mecanismos**: O software trabalha com dois **mecanismos** (engine = máquina/motor em inglês), ou seja, dois programas de verificação de vírus independentes entre si. Cada mecanismo, por si só, já protegeria contra vírus, em alta escala, mas, exatamente a combinação de ambos os mecanismos, oferece os melhores resultados. Em computadores antigos e lentos, é possível, mediante a utilização de apenas um único mecanismo, acelerar a verificação de vírus; no entanto, via de regra, deve-se manter a configuração **Ambos os mecanismos**.
- **Arquivos infectados**: O software encontrou um vírus? Na configuração padrão, o software pergunta o que você deseja fazer com o vírus e o arquivo infectado. Quando desejar executar sempre a mesma ação, poderá definir isto aqui. A máxima segurança para os seus dados é oferecida pela configuração **Desinfectar (se não for possível: para quarentena) quarentena))**.
- **Pastas infectadas**: Defina aqui se as **pastas** (por exemplo, arquivos com a extensão **RAR**, **ZIP** ou também **PST**) deverão ser tratadas de forma diferente dos arquivos normais. No entanto, observe que mover um arquivo compactado para a quarentena pode danificá-lo, de forma que ele também não poderá mais ser usado após movê-lo de volta. Por essa razão, em caso de pastas infectadas, recomenda-se decidir caso a caso e selecionar **Perguntar as ações desejadas**.
- **Em caso de sobrecarga suspender a verificação de vírus**: Normalmente, uma verificação de vírus só pode ocorrer quando seu computador não estiver sendo utilizado. Se você precisar utilizar o computador, a verificação de vírus é pausada para que o computador esteja disponível na velocidade comum. A verificação de vírus também é executada durante as suas pausas no trabalho.

Exceções

Clicando no botão **Exceções**, você pode excluir determinadas unidades, diretórios e arquivos da verificação e, dessa forma, acelerar significativamente o reconhecimento de vírus. Para isso, proceda da seguinte forma:

1. Clique no botão **Exceções**.

2. Clique, na janela **Exceções para a verificação manual do computador**, em **Novo**.

3. Selecione agora se deseja que a exceção seja aplicada a uma unidade de disco, um diretório, arquivo ou tipo de arquivo.

4. Então, selecione abaixo o diretório ou a unidade que deseja proteger. Para proteger arquivos, digite o nome completo do arquivo no campo de entrada na máscara de arquivos. Aqui também é possível trabalhar com **Espaços reservados**.

   A forma de funcionamento dos Espaços reservados é a seguinte:

   - O **ponto de interrogação** (?) é substituto para caracteres individuais.
   - * O **asterisco** (*) é substituto para seqüências de caracteres inteiras.

   Para, por exemplo, proteger todos os arquivos com a extensão **.sav** , digite ***.sav**. Para proteger uma seleção especial com nomes de arquivo sequenciais, (p.ex., text1.doc, text2,doc, text3.doc), digite, por exemplo, **text?.doc**.

Esse processo pode ser repetido quantas vezes desejar e também, é possível excluir ou modificar novamente as exceções existentes.

> **Utilizar as exceções também para a verificação em modo ocioso**: Enquanto na verificação manual de vírus o computador é objetivamente verificado quanto a vírus e não deve ser utilizado para outras tarefas, a **Verificação em modo ocioso** é uma verificação inteligente de vírus, em que todos os arquivos do seu computador são sempre verificados se já não estão infectados com um vírus. A verificação em modo ocioso trabalha como um protetor de tela, sempre que o seu computador não estiver sendo usado, e para imediatamente assim que você continua a trabalhar para garantir um desempenho ideal. Aqui é possível estabelecer se, também para a verificação em modo ocioso, os arquivos de exceção ou os diretórios de exceção devem ser definidos.

Avançado

Um clique no botão **Avançado** possibilita efetuar configurações avançadas para a verificação de vírus. Na maioria dos casos, é totalmente suficiente utilizar as configurações padrão.

- **Tipos de arquivos**: Aqui é possível definir quais os tipos de arquivos em que o software deverá examinar a existência de vírus. A seleção da opção **Somente arquivos de programa e documentos** aumenta a velocidade.
- **Heurística**: Na análise heurística, os vírus não são reconhecidos somente por meio dos bancos de dados de vírus que você obtém a cada atualização do software antivírus mas também através de determinadas características típicas de vírus. Esse método é mais uma vantagem de segurança, no entanto, em raros casos, pode levar a um alarme falso.
- **Verificar pastas (compactadas)**: A verificação de dados em arquivos compactados (reconhecidos através das extensões de arquivo **ZIP**, **RAR** ou também **PST**) demanda muito tempo e normalmente pode ser ignorada quando a Sentinela de vírus estiver, em geral, ativada no sistema. Para aumentar a velocidade da verificação de vírus, você pode limitar o tamanho das pastas, que serão verificadas, para um determinado valor em megabytes.
- **Verificar pastas de e-mail**: Aqui é possível definir se também os seus arquivos de e-mail devem ser verificados quanto a infecções.
- **Verificar áreas do sistema**: As áreas de sistema (p.ex., setores de boot) do seu computador não devem ser ignoradas no controle de vírus.
- **Verificar Discador/Spyware/Adware/Riskware**: Com esta função, o seu sistema pode ser verificado também quanto a **Discadores** e outros softwares maliciosos (**Spyware**, **Adware** e **Riskware**). Aqui, trata-se de programas que estabelecem caras e indesejadas conexões à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, que p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.
- **Verificar a existência de Rootkits**: Os **Rootkits** tentam escapar dos métodos comuns de detecção de vírus. É sempre recomendável um controle adicional desses softwares maliciosos.
- **Verificar somente arquivos novos ou alterados**: Se você ativar esta função, serão verificados somente os arquivos que não são alterados há muito tempo e que antes tinham sido reconhecidos como inofensivos. Isso leva a um ganho de desempenho no trabalho diário – sem risco de segurança.
- **Criar relatório**: Neste campo de marcação, é possível definir se o software deve criar um registro sobre o processo de verificação de vírus. Isto pode ser visto na área **Registros**.

Atualizações

Se a atualização do software ou das assinaturas de vírus não funcionar pela internet, você pode fornecer todas as informações necessárias nesta área para possibilitar uma atualização automática. Informe aqui, nas opções, os seus dados de acesso (**nome de usuário** e **senha**) que você recebeu por e-mail no registro on-line do seu software. Com esses dados, você será reconhecido pelo servidor de atualização G Data e as atualizações podem ocorrer de forma completamente automática.

> Se você adquiriu uma licença nova e quer ativá-la, selecione **Registrar no servidor**. As configurações da Internet mostram opções especiais que são necessárias apenas em alguns casos excepcionais (servidor proxy, outra região). Você deve ativar a verificação de versão apenas temporariamente quando tiver dificuldades na atualização das assinaturas de vírus.

Atualizar assinaturas de vírus automaticamente

Caso você não queira que o software G Data cuide da atualização das assinaturas de vírus automaticamente, você pode desmarcar a caixa aqui. No entanto, a desativação significa um alto risco de segurança e deve ser efetuada apenas em casos excepcionais. Se o intervalo entre as atualizações for muito pequeno para você, você pode adequá-lo individualmente e determinar, por exemplo, que estas sejam efetuadas apenas com o início da conexão à internet. Esta seleção faz sentido, por exemplo, em computadores que não têm uma conexão permanente com a internet.

> **Criar relatório**: Se a marcação for colocada aqui, toda a atualização das assinaturas de vírus será integrada no registro, o que pode ser visualizado nas funções adicionais do software G Data (na **SecurityCenter** em **Mais** > **Registros**). Além desses registros, você encontra neles, por exemplo, informações sobre descobertas de vírus e outras ações que foram efetuadas pelo programa.

Registrar no servidor

Se você ainda não tiver registrado o seu software G Data poderá fazê-lo agora e inserir seu número de registro e os dados do cliente. Você encontra o **número de registro**, dependendo do tipo do produto, por ex., na contracapa do manual de utilização, no e-mail de confirmação no download do software ou na capa do CD.

> **Através da inserção do número de registro, o produto é ativado**

Clique agora no botão **Log-in** e os seus dados de acesso serão gerados no servidor de atualização. Se o registro tiver sido realizado com sucesso, aparecerá uma tela de informações com a observação **O registro foi concluído com sucesso**, a qual pode ser fechada com o botão Fechar.

> **Atenção**: Para a sua documentação e possíveis reinstalações do software, os seus **dados de acesso** também serão enviados por e-mail. Por isso, verifique se no seu registro on-line consta o seu endereço de e-mail correto, caso contrário, os dados de acesso não serão disponibilizados.

Para finalizar, os dados de acesso serão automaticamente aplicados na máscara de entrada original e então você poderá atualizar assinaturas de vírus através da Internet.

> **Não consegue se registrar no servidor?** Se você não puder se registrar no servidor, talvez ele esteja em um servidor proxy. Clique no botão **Configurações da Internet**. Aqui será possível efetuar as configurações para sua conexão à Internet. Normalmente, em caso de problemas com a atualização das assinaturas de vírus, você deve primeiro verificar se consegue acessar a Internet com um navegador (por ex., Internet Explorer). Se você não conseguir criar uma conexão à internet, o problema provavelmente está na área da conexão à internet, e não nas informações do servidor proxy.

Configurações da Internet

Se utilizar um Servidor proxy, coloque a marcação em **Utilizar servidor proxy** Essas configurações só devem ser alteradas quando a atualização das assinaturas de vírus não funcionar. Se for necessário, fale com o administrador do sistema ou com o provedor de Internet sobre o endereço proxy. Se necessário, poderá inserir aqui os dados de acesso para o servidor proxy.

> **Servidor proxy**: Um servidor proxy junta consultas às redes e as distribui aos seus computadores conectados. Se utilizar o seu computador em uma rede da empresa, por exemplo, pode ser que você se conecte à rede através de um servidor proxy. Geralmente, em problemas com a atualização das assinaturas de vírus, você deverá verificar primeiramente se consegue se conectar à rede através de um servidor da internet. Se você não conseguir criar uma conexão à internet, o problema provavelmente está na área da conexão à internet, e não nas informações do servidor proxy.

Proteção da web

Aqui podem ser feitas as seguintes configurações.

- **Processar conteúdo da Internet (HTTP)**: Nas opções de proteção da Web, você pode definir que a existência de vírus em todo o **conteúdo da Web por HTTP** seja verificada já na navegação. O conteúdo infectado da Web não é executado e as respectivas páginas não são exibidas. Para isso, coloque a marcação em **Processar conteúdo da Internet (HTTP)**.

> Se você não desejar permitir a verificação dos conteúdos da Internet, **a sentinela de vírus** entra naturalmente em ação quando arquivos infectados forem executados. Ou seja, o seu sistema está protegido mesmo sem a verificação do conteúdo da Internet enquanto a sentinela estiver ativa.

> Você pode definir determinadas páginas da internet como exceções quando avaliá-las como inofensivas. Para isso, leia o capítulo **Definir exceções** Com o botão **Avançado**, você pode efetuar mais configuração sobre o tratamento de conteúdos da internet. Para os navegadores **Internet Explorer** e **Firefox**, existem plug-ins para efetuar as definições das exceções acima mencionadas diretamente no navegador, de forma mais confortável.

- **Proteção contra phishing:** Com os chamados **Phishing** os trapaceiros da Internet, tentam direcionar os clientes de um determinado banco ou loja, para um site falsificado e lá, roubar seus dados. O Filtro da Web recebe on-line e constantemente, as mais recentes informações sobre novos sites de phishing e os suprime automaticamente. A ativação dessa opção de Proteção contra phishing é altamente recomendada.
- **Enviar endereços de páginas da Internet infectadas**: Através desta função, você pode - naturalmente de forma anônima - informar automaticamente as páginas da Internet que foram consideradas como perigosas pelo software. Com isso você otimiza a segurança para todos os usuários.
- **Processar conteúdo de mensagens instantâneas**: Como vírus e outros programas maliciosos podem ser propagados também através de ferramentas de mensagens instantâneas, o software pode impedir a exibição e o download de dados infectados em primeiro plano. Se no aplicativo de mensagens instantâneas você não usar as portas padrão, poderá informar em **Avançado** as respectivas **portas**.
- **Inserção no aplicativo Messenger**: Se você utilizar o **Microsoft Messenger** ou o **Trillian**, é possível, colocando a marcação para o respectivo programa, definir um menu contextual no qual você poderá verificar a existência de vírus diretamente em arquivos suspeitos.

Definir exceções

Para colocar uma página da Internet como exceção na Whitelist, proceda da seguinte forma:

1. Clique no botão **Definir exceções**. A janela Whitelistserá exibida. Aqui serão exibidos os sites da web classificados como seguros e aqui inseridos.

2. Para adicionar outros sites da Internet, clique agora no botão Novo. Uma máscara de entrada será exibida. Em **URL**, insira o endereço do site (por exemplo, www.umsiteseguro.com.br) e, em **Comentário**, adicione uma nota, se necessário, descrevendo a razão de ter colocado o site. Confirme a inserção com um clique em OK.

3. Confirme então com um clique em OK todas as alterações feitas na Whitelist.

Para excluir novamente um site da whitelist, marque-o na lista com o mouse e clique no botão Para excluir.

Avançado

Aqui é possível definir quais **números de porta de servidor** devem ser monitorados pela proteção da Web. Normalmente, para um monitoramento do navegador normal, é suficiente aqui o número da porta 80.

- **Evitar ultrapassar limite de tempo no navegador**: Como o software processa o conteúdo da Internet antes de sua exibição no navegador da Internet, e esse, dependendo dos resultados dos dados necessita de um certo tempo, pode ocorrer que uma mensagem de erro apareça no navegador da Internet, pelo não recebimento imediato dos dados, devido a estarem sendo verificados. Com a colocação da marcação no campo **Evitar ultrapassar limite de tempo no navegador**, evita-se uma mensagem de erro e, assim que a existência de vírus for verificada em todos os dados do navegador, esses serão transmitidos normalmente para o navegador da Internet.

- **Limite de tamanho para downloads**: Através desta opção, é possível impedir uma verificação de HTTP para conteúdos da Web muito grandes. O conteúdo é verificado pela sentinela de vírus assim que qualquer rotina maliciosa ficar ativa. A vantagem dessa limitação de tamanho é de que ao navegar na Web, nenhum retardo ocorre devido ao controle de vírus.

Verificação de e-mail

Com a verificação de e-mail é possível verificar a existência de vírus em e-mails de entrada e saída, seus anexos e, desativar possíveis infecções diretamente na origem. Se um vírus for encontrado, o software é capaz de excluir diretamente anexos de arquivos ou reparar arquivos infectados.

No **Microsoft Outlook** a verificação de e-mail é realizada através de um **Plug-In**. Ele oferece a mesma proteção que as funções de proteção orientadas a **POP3/IMAP** dentro das opções do **AntiVirus**. Após a instalação desse Plug-in, você encontrará no menu do **Outlook**, **Ferramentas**, a função **Verificar individualmente a existência de vírus na pasta**, com a qual poderá verificar a existência de vírus em suas pastas de e-mail.

E-mails de entrada

- **No caso de uma infecção**: Aqui você pode definir o que deve ocorrer na detecção de um e-mail infectado. Dependendo do fim para o qual o seu computador é utilizado, diferentes configurações são recomendáveis. Por via de regra, a configuração **Desinfectar (se não for possível: excluir anexo/texto)** é a recomendada.
- **Verificar e-mails recebidos**: Com a ativação dessa opção, a existência de vírus é verificada em todos os **e-mails** que entram no computador durante o seu trabalho.
- **Verificar e-mails não lidos no início do programa (somente para o Microsoft Outlook)**: Essa opção serve para controlar a existência de vírus em e-mails que o acessam durante a sua conexão com a Internet. Portanto, assim que você abre o **Outlook**, todos os e-mails não lidos na pasta caixa de entrada e suas sub-pastas, serão controlados.
- **Anexar relatório aos e-mails recebidos e infectados**: Se tiver ativado a opção de relatório, aparecerá, em caso de uma detecção de vírus, na linha de assunto do e-mail infectado o aviso **VÍRUS** e, no começo do texto do e-mail, aparece a mensagem **Atenção! Este e-mail contém os seguintes vírus:** seguido pelo nome do vírus e a informação se o vírus foi excluído ou se o arquivo infectado pôde ser reparado.

E-mails de sada

- **Verificar e-mails antes do envio**: Para que você não encaminhe vírus inadvertidamente, o software oferece também a possibilidade de verificar a existência de vírus em seus e-mails antes do envio. Se você realmente desejar (inadvertidamente) enviar um vírus, aparece a mensagem **O e-mail [Linha de assunto] contém os seguintes vírus: [Virusname]**. O e-mail não pode ser enviado e o respectivo e-mail não será enviado.

Opções de varredura

- **Utilizar mecanismos:**: O software trabalha com dois mecanismos antivírus; duas unidades operacionais de análise independentes uma da outra. Em princípio, a utilização dos dois mecanismos é a garantia para os resultados ideais da profilaxia de vírus.

- **OutbreakShield**: Através dessa opção você ativa a OutbreakShield. O software cria, com a OutbreakShield ativada, somas de teste de e-mails, compara-as com as blacklists antispam constantemente atualizadas na Internet e, com isso, é capaz de reagir a um envio de e-mails em massa antes que existam as respectivas assinaturas de vírus. A OutbreakShield consulta na Internet sobre acumulações especiais de e-mails suspeitos e fecha, quase em tempo real, a brecha que existe entre o começo de um e-mail em massa e seu combate através de assinaturas de vírus adaptadas especialmente. A OutbreakShield está integrada no bloqueador de vírus de e-mail.

Avançado

Se na utilização do seu programa de e-mail você não usar as **portas padrão**, poderá informar em **Número da porta do servidor**, também a **porta** que utiliza para e-mails de entrada ou saída. Ao clicar no botão **Padrão**, é possível restaurar novamente e de forma automática o número da porta padrão. Você também pode inserir diversas portas. Separe-as respectivamente por uma vírgula.

O **Microsoft Outlook** é protegido por um Plugin especial, através do qual é possível diretamente do **Outlook** verificar pastas e e-mails. Para verificar a existência de vírus em um e-mail ou pasta no Outlook, selecione na barra de menu do Outlook o comando **Ferramentas > Verificar a existência de vírus na pasta** e a pasta de e-mail selecionada será verificada.

Como o software processa os e-mails de entrada oportunamente antes do próprio programa de e-mail, em grandes quantidades de e-mail ou conexões lentas, poderá aparecer uma mensagem de erro no programa de e-mail, pois esse não recebe imediatamente os dados dos e-mails que estão sendo verificados pelo software quanto a vírus. Com a ativação do campo de marcação em **Evitar ultrapassar limite de tempo no servidor de e-mail**, evita-se uma mensagem de erro do programa de e-mail e, assim que a existência de vírus for verificada em todos os dados de e-mails, esses serão encaminhados normalmente pelo software para o programa de e-mail.

Verificações automáticas de vírus

Aqui é possível ativar ou desativar a **Verificação em modo ocioso**. Além disso, você pode, em vez disso ou adicionalmente, examinar de forma periódica o seu computador ou as áreas do computador quanto a infecções. Por exemplo, você pode executar essas verificações nos períodos em que o seu computador não estiver sendo utilizado.

Verificações de vírus diferentes: Em muitos casos, é suficiente quando o computador é verificado em modo ocioso. Com o botão **Novo**, você pode criar diferentes verificações automáticas de vírus e independentes entre si. Por exemplo, na pasta **Downloads**, você pode configurar que a sua coleção de MP3 seja verificada apenas uma vez por mês.

Geral

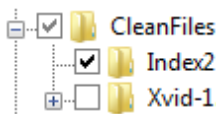
Aqui você determina o nome da verificação automática de vírus recentemente configurada. Para a diferenciação, recomenda-se nomes significativos, como por exemplo, **Discos rígidos locais (verificação semanal)** ou **Pastas (verificação mensal)**.

Se você colocar uma marcação em **Desligar o computador após a conclusão da tarefa**, o computador será desligado automaticamente após a conclusão da verificação automática de vírus. Isto é útil quando desejar, p. ex., executar a verificação de vírus após o trabalho no escritório.

Tarefa: Cada uma das ordens automáticas definidas para a verificação do computador ou de determinadas áreas é denominada tarefa.

Escopo da análise

Defina aqui se a verificação de vírus deverá ser feita nos **Discos rígidos locais**, se as área **Memória** e **inicialização automática** devem ser testadas ou se deseja apenas verificar determinados **Diretórios** e **Arquivos**. Se for esse o caso, informe os diretórios desejados através do botão **Opção** .

> **Selecionar diretórios/arquivos**: Na árvore de diretórios (à esquerda), clicando nos sinais (+), é possível abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo. Cada diretório ou arquivo com uma marcação será verificado pelo software. Se nem todos os arquivos tiverem que ser verificados em um diretório, haverá uma marcação em cinza nesse diretório.

Programação

Nessa guia, é possível definir quando e em que ritmo a respectiva tarefa deverá ocorrer. Em **Executar**, insira uma predefinição que você pode detalhar em **Período**. Se você selecionar **Na inicialização do sistema**, as predefinições da programação continuarão e o Software executará a verificação sempre que o seu computador for reinicializado.

- **Executar a tarefa se o computador não estiver ligado na hora de início**: Com a ativação desta opção, as verificações automáticas de vírus não executadas serão feitas automaticamente assim que o computador for reinicializado.

- **Não executar com a bateria**: Para não reduzir a duração da bateria desnecessariamente, você pode, por ex., definir para **notebooks** que as verificações automáticas de vírus ocorram somente quando o computador portátil estiver conectado à rede elétrica.

Configurações de verificação

Nessa área você pode definir com que configurações a verificação automática de vírus deverá ocorrer.

- **Utilizar mecanismos**: O software trabalha com dois **mecanismos**, ou seja, dois programas de verificação independentes entre si. Cada mecanismo, por si só, já protegeria contra vírus, em alta escala, mas, exatamente a combinação de ambos os mecanismos, oferece os melhores resultados. Em computadores antigos e lentos, é possível, mediante a utilização de apenas um único mecanismo, acelerar a verificação de vírus; no entanto, via de regra, deve-se manter a configuração **Ambos os mecanismos**.
- **Arquivos infectados**: O software encontrou um vírus? Na configuração padrão, o software pergunta o que você deseja fazer com o vírus e o arquivo infectado. Quando desejar executar sempre a mesma ação, poderá definir isto aqui. A máxima segurança para os seus dados é oferecida pela configuração **Desinfectar (se não for possível: para quarentena) quarentena))**.
- **Pastas infectadas**: Defina aqui se a **pasta** (por exemplo, arquivos com a extensão **RAR**, **ZIP** ou também **PST**) deverão ser tratados de forma diferente dos arquivos normais. No entanto, observe que mover um arquivo compactado para a quarentena pode danificá-lo, de forma que ele também não poderá mais ser usado após movê-lo de volta. Por essa razão, em caso de pastas infectadas, recomenda-se decidir caso a caso e selecionar **Perguntar as ações desejadas**.

Além disso, defina através do clique no botão **Avançado** que verificações adicionais deverão ser executadas pelas verificações de vírus adicionais.

Na maioria dos casos, é totalmente suficiente utilizar as configurações padrão.

- **Tipos de arquivos**: Aqui é possível definir quais os tipos de arquivos em que o software deverá examinar a existência de vírus.
- **Heurística**: Na análise heurística, os vírus não são reconhecidos somente por meio dos bancos de dados de vírus que você obtém a cada atualização do software, mas também através de determinadas características típicas de vírus. Esse método é mais uma vantagem de segurança, no entanto, em raros casos, pode levar a um alarme falso.

- **Verificar pastas (compactadas)**: A verificação de dados em arquivos compactados (reconhecidos através das extensões de arquivo **ZIP**, **RAR** ou também **PST**) demanda muito tempo e normalmente pode ser ignorada quando a **Sentinela de vírus** estiver, em geral, ativada no sistema. Ela reconhece na descompactação um vírus oculto até o momento e, impede automaticamente a sua propagação.
- **Verificar pastas de e-mail**: Aqui é possível definir se também os seus arquivos de e-mail devem ser verificados quanto a infecções.
- **Verificar áreas do sistema**: As áreas de sistema (p.ex., **setores de boot**) do seu computador não devem ser ignoradas no controle de vírus.
- **Verificar Discador/Spyware/Adware/Riskware**: Com esta função, o seu sistema pode ser verificado também quanto a **Discadores** e outros softwares maliciosos (**Spyware**, **Adware** e **Riskware**). Aqui, trata-se de programas que estabelecem caras e indesejadas conexões à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, que p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.
- **Verificar a existência de Rootkits**: Os **Rootkits** tentam escapar dos métodos comuns de detecção de vírus. É sempre recomendável um controle adicional desses softwares maliciosos.
- **Criar relatório**: Neste campo de marcação, é possível definir se o software deve criar um registro sobre o processo de verificação de vírus. Isto pode ser visto na área **Registros**.

Conta do usuário

Aqui é possível inserir a conta de usuário na qual a verificação de vírus deverá ocorrer. Essa conta será necessária para o acesso à unidade de rede.

Saiba mais

Aqui você pode obter informações sobre funções importantes do programa do software.

BootScan

O **BootScan** ajuda a combater vírus que se aninharam em seu computador antes da instalação do software antivírus e que, possivelmente, podem impedir a instalação do G Data software. Para isso, existe uma versão especial do programa do Software que pode ser executada já antes da inicialização do Windows.

O que significa um processo de inicialização? Quando você liga o seu computador, normalmente, o sistema operacional Windows é iniciado automaticamente. Este processo se chama **Dar um boot**. Existe também a possibilidade de iniciar outros programas automaticamente, ao invés do sistema operacional Windows. Para verificar a existência de vírus no seu computador antes da inicialização do Windows, a G Data disponibiliza, adicionalmente à versão do Windows, uma versão especial com capacidade de boot.

Como eu cancelo um BootScan? Se, após uma reinicialização, o seu computador não mostrar o habitual ambiente do Windows, mas uma interface especial do software G Data, isso não deverá ser motivo para preocupações. Se não tiver planejado nenhum BootScan, basta selecionar com as teclas de seta o registro **Microsoft Windows** e clicar em **Voltar**. O Windows inicializará normalmente, sem o BootScan.

Se desejar executar um **BootScan**, proceda da seguinte forma:

1a **BootScan com o CD do programa**: Utilize o CD do programa da G Data e faça com ele o boot no seu computador. - Insira o CD da G Data na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

1b **Faça o BootScan com o software G Data descarregado da Internet**: Através do registro Criar CD de boot da **G Data** no grupo de programas da **G Data** (*ícone do Windows na barra de tarefas > Todos os programas > Software G Data > Criar CD de boot*), você grava um novo BootCD.

Insira o seu próprio BootCD gravado na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

Se você usa o **Windows XP**, pode acontecer que, na tentativa de criar um BootCD, receba uma mensagem que o **IMAPI 2.x** não está instalado. Trata-se de uma atualização do Microsoft para sistemas operacionais antigos que é necessária para gravar mídias de dados. Você pode descarregar a atualização necessária diretamente da página inicial da Microsoft e instalá-la.

1c **Você tem uma versão especial para netbook do software G Data em um pen drive?** Aqui é possível executar o BootScan diretamente através do pen drive. No entanto, para isto, o seu netbook terá que ser capaz de dar o boot a partir de um pen drive.

Conecte o **G Data pen drive** com o seu netbook. Na janela de inicialização aberta, clique em **Cancelar** e desligue o Netbook.

Após a primeira etapa o BootScan para as três variações tem o mesmo procedimento:

2 Reinicialize o computador. O menu de inicialização do G Data **BootScan** aparece.

3 Com as setas, selecione a opção G Data**BootCD** e confirme a seleção com **Enter**. Um sistema operacional Linux será iniciado pelo CD e aparecerá uma versão especial da G Data para BootScans.

Se tiver problemas com a visualização da interface do programa, reinicialize o seu computador e selecione a opção G Data **BootCD – Alternativo**.

4 O programa irá sugerir agora a atualização das assinaturas de vírus.

Se você utiliza uma versão do software G Data que é compatível com as funções de backup, aqui você tem a possibilidade adicional de iniciar diretamente a reprodução de backups de seus dados armazenados.

5 Clique agora em **Sim**. Para poder executar a atualização, você deve inserir seus dados de acesso já recebidos ou seu número de registro. Depois disso, você pode executar a atualização. Assim que os dados tiverem sido atualizados na Internet, aparecerá o aviso **Atualização concluída**. Saia agora da tela de atualização clicando no botão **Fechar**.

A **atualização automática na Internet** é disponibilizada quando for utilizado um **roteador** que atribua endereços IP automaticamente (**DHCP**). Se não for possível a atualização na Internet, o **BootScan** poderá ser executado também com as assinaturas de vírus antigas. No entanto, nesse caso, após a instalação do software G Data , você deverá executar o mais rápido possível um novo BootScan com dados atualizados.

6 Agora você verá a interface do programa. Clique no registro **Verificar computador** e o seu computador será agora verificado quanto à existência de vírus e softwares maliciosos. Este processo pode levar uma hora ou mais, dependendo do tipo de computador e tamanho do disco rígido.

7 Se o software G Data encontrar vírus, remova-os com a ajuda da opção sugerida no programa. Após a remoção bem-sucedida do vírus, o arquivo original ficará novamente disponível.

8 Após concluir a verificação de vírus, saia do sistema clicando no x (no canto superior direito da janela).

9 Remova o CD do software G Data da unidade assim que a sua unidade for aberta ou desconecte o pen drive G Data do seu netbook.

10 Desligue novamente o seu computador e o reinicie. Agora, o seu computador inicializará novamente com o sistema operacional Windows padrão e você terá a garantia de poder instalar o software normal da G Data em um sistema sem vírus.

O que faço quando meu computador não faz o boot a partir do CD-ROM?

Se não for possível o boot a partir do CD/DVD-ROM, pode ser que essa opção precise primeiro ser ativada. Isto é feito na chamada **BIOS**, um sistema, que é inicializado automaticamente antes do sistema operacional Windows. Para fazer alterações na BIOS, execute as seguintes etapas:

1. Desligue o seu computador.
2. Reinicialize o computador. Normalmente, você consegue acesso à configuração da BIOS, ao iniciar (= Boot) o computador você pressionar a tecla **Del** (algumas vezes também a tecla **F2** ou **F10**).
3. A forma de alteração individual na configuração da BIOS é diferente de computador para computador. Leia para isto, a documentação do seu computador. Em resumo, a sequência do boot deve ser **CD/DVD-ROM:, C:** ou seja, a unidade de CD/DVD-ROM será o **1st Boot Device** e a partição do disco rígido, com o seu sistema operacional Windows, será o **2nd Boot Device**.
4. Salve as alterações e reinicie o seu computador. Agora o computador estará pronto para um BootScan.

O que faço quando o meu netbook (ou também PC desktop/ notebook) não faz o boot a partir do pen drive?

Se o seu computador não fizer o boot automaticamente a partir do pen drive, execute as seguintes etapas:

1. Desligue o seu computador.
2. Insira o G Data **pen drive** em uma **porta USB** livre do seu computador.
3. Ligue o seu computador.
4. Durante a inicialização, pressione a tecla **F2**, para chegar na **BIOS** do computador.
5. A interface da BIOS será exibida com uma barra de menu, onde você pode selecionar o menu **Boot** com as teclas de seta (para direita/esquerda). Agora, pressione **Enter**.
6. Você terá, então, a possibilidade de selecionar o registro **Hard disc drives** através das teclas de seta (para cima/baixo). Agora, pressione **Enter**.
7. Selecione agora o registro **USB** de forma que **1st Drive = USB** apareça em primeiro lugar (teclas **Enter** e de setas).

8. Pressione **F10**, para salvar e fechar a BIOS. O seu computador poderá agora fazer o boot a partir do pen drive.
9. Reinicialize o computador. Agora o computador estará pronto para um BootScan.

Ícone G Data

O software G Data protege o seu computador permanentemente contra vírus e softwares maliciosos. Para que você possa ver que a proteção está ativa, um ícone é exibido na barra de tarefas ao lado do relógio.

Este ícone G Data indica que está tudo em ordem e que a proteção do seu computador está ativa.

Caso a sentinela tenha sido desativada ou existam outros problemas, o ícone G Data exibirá um sinal de aviso. Nesse caso, você deverá iniciar o software G Data o mais rápido possível e verificar as configurações.

Quando o softwareG Data executa um download de dados da Internet, ele também indica isso através de um ícone especial.

Se clicar no ícone com o botão direito do mouse, aparece um menu contextual com o qual se pode controlar os aspectos de segurança fundamentais do software.

As seguintes funções estão disponíveis:

- **G Data** : Com essa opção, ativa-se a **SecurityCenter** e é possível efetuar as configurações para a sentinela de vírus. As possibilidades existentes na SecurityCenter podem ser consultadas no capítulo: **SecurityCenter**
- **Desativar sentinela**: Com esta opção, é possível desativar a **Sentinela de vírus**, em caso de necessidade, e também ativá-la novamente. Isso pode ser útil, p.ex, quando uma grande quantidade de dados em seu disco rígido é copiada de um local para outro ou para rodar processos de exibição que ocupam muito espaço na memória (copiar DVDs e outros). A sentinela de vírus só deve ser desativada quando for realmente necessário e, deve-se ter a certeza de que o sistema durante esse período, se possível, não esteja conectado à Internet ou possa acessar dados novos e não verificados (p.ex, através de CDs, DVDs, placas de memória ou dispositivos USB).

- **Desativar firewall**: Se você usar uma versão do software G Data com firewall integrado, também é possível desativar o **firewall** através do menu contextual, caso necessário. O seu computador estará ainda conectado à Internet e a outras redes, mas não estará protegido contra ataques ou espionagem.
- **Desativar piloto automático**: O **Piloto automático** é uma parte do **Firewall** e decide de forma independente que solicitações e contatos o seu computador deve aceitar ou não através da rede ou Internet. O piloto automático é ideal para uma utilização normal e deverá ser deixado sempre ativado. Como o firewall, o piloto automático está disponível nas versões selecionadas do software G Data.
- **Atualização de vírus**: Um software antivírus deve estar sempre atualizado. Naturalmente, você pode solicitar que atualização dos dados seja executada automaticamente pelo software. No entanto, se você precisar urgentemente de uma atualização, poderá iniciá-la através do botão **Atualização de vírus**. Para saber a utilidade de uma atualização de vírus, pode ser lido no capítulo: **Atualizações**
- **Estatística**: Essa opção permite exibir uma estatística sobre os eventos de verificação.

Verificação de vírus

Com a verificação de vírus, você verifica se o seu computador foi infectado por softwares maliciosos. Quando você inicia a verificação de vírus, esse controla cada arquivo no seu computador, quanto a possibilidade desse poder infectar outros arquivos ou se o próprio já está infectado. Se vírus ou outros softwares maliciosos forem encontrados em uma verificação de vírus, existem diversas possibilidades como o vírus pode ser removido ou tornado inofensivo.

1 Inicie a verificação de vírus. Leia o procedimento para isso no capítulo: **Proteção AntiVirus**

2 Será iniciada uma verificação de seu computador quanto a infecção por vírus. Além disto, é aberta uma janela onde você obtém informações sobre o status da verificação.

Uma barra de progresso na parte superior da janela, indica o progresso da verificação no seu sistema. Já durante a verificação de vírus você terá diversas possibilidades para influenciar o andamento da verificação de vírus:

- **Em caso de sobrecarga suspender a verificação de vírus**: Através desse campo de opções, você pode definir que o software espere com a verificação de vírus, até que as outras atividades no computador tenham sido concluídas.
- **Desligar computador após a verificação de vírus**: Esta função é bastante prática, quando você desejar deixar a verificação de vírus rodando durante a noite ou após o expediente. Assim que a verificação de vírus do software G Data for finalizada, o seu computador será desligado.
- **Pastas protegidas por senha**: Enquanto uma pasta compactada for protegida por senha, o softwareG Data não pode verificar os arquivos desta pasta. Se colocar uma marcação aqui, o software antivírus o informa quais pastas compactadas protegidas por senha não pôde verificar. Contanto que essa pasta não seja descompactada, um vírus ali contido não representa nenhum risco para o seu sistema.
- **Acesso negado**: Em geral, existem arquivos no Windows utilizados exclusivamente pelos aplicativos e que por isso, não podem ser verificados enquanto esses aplicativos estiverem sendo executados. Portanto, o melhor é que nenhum outro programa esteja sendo executado em seu sistema durante uma verificação de vírus. Ao colocar aqui uma marcação, os dados não verificados serão exibidos.

3a Assim que o seu sistema estiver livre de vírus, você poderá, após o término da verificação, sair da janela do assistente, através do botão **Fechar**.

O seu sistema terá sido verificado e estará livre de vírus.

3b Para o caso de vírus e outros programas maliciosos terem sido encontrados, você terá a possibilidade, agora, de decidir como deseja proceder com as detecções de vírus. Normalmente, basta clicar no botão **Executar ações**.

O softwareG Data utiliza então uma configuração padrão (*desde que você não tenha configurado isso diferentemente nas configurações em **AntiVirus > Verificação manual de vírus para arquivos e pastas infectadas***) e desinfecta os arquivos afetados, ou seja, ele os repara de forma que possam ser novamente utilizados sem restrições e não sejam mais perigosos para o seu computador.

Se uma desinfecção não for possível, o arquivo será colocado em quarentena, ou seja, ele será codificado e movido para uma pasta extremamente segura, onde não poderá mais causar danos.

Se esse arquivo infectado ainda for necessário, ele poderá, em casos excepcionais, ser novamente retirado da área da quarentena e utilizado.

O seu sistema terá sido verificado e estará livre de vírus.

3c Quando os arquivos/objetos infectados forem conhecidos e você puder diferenciar quais deles talvez não sejam mais necessários, existe a possibilidade de reagir de forma bastante individual à cada detecção de vírus.

Na listagem das detecções de vírus, é possível, na coluna **Ação**, definir, para cada arquivo infectado, o que deverá ocorrer com o mesmo.

- **Somente registrar**: Na visualização **Registros** a infecção é relacionada. No entanto, não é feita a reparação ou exclusão do arquivo afetado. **Atenção: Quando um vírus for somente registrado ele permanece ativo e perigoso.**
- **Desinfectar (se não for possível: somente registrar)**: Aqui, tenta-se remover o vírus de um arquivo infectado. Se isso não for possível sem danificar o arquivo, o vírus será registrado e você poderá cuidar disso mais tarde, através do registro. **Atenção: Quando um vírus for somente registrado ele permanece ativo e perigoso.**
- **Desinfectar (se não for possível: para quarentena)**: Esta é a configuração padrão. Aqui, tenta-se remover o vírus de um arquivo infectado, se não for possível sem danificar o arquivo, esse é movido para a **Quarentena**. Para isso, leia também o capítulo **Como funciona a quarentena?**
- **Desinfectar (se não for possível: Excluir arquivo**: Aqui tenta-se remover o vírus de um arquivo afetado. Se isso não for possível, o arquivo será excluído. Esta função só deve ser utilizada quando nenhum dado importante existir no seu computador. Uma exclusão de arquivos infectados pode, na pior das hipóteses fazer com que o seu Windows não mais funcione e que uma reinstalação seja necessária.

- **Mover arquivo para a quarentena**: Os arquivos infectados são movidos diretamente para a **Quarentena**. Na quarentena, os arquivos são armazenados criptografados. Ou seja, o vírus não pode causar nenhum dano e o arquivo infectado continuará existente para eventuais tentativas de reparação. Leia para isso também o capítulo: **Como funciona a quarentena?**
- **Excluir arquivo**: Esta função só deve ser utilizada quando nenhum dado importante existir no seu computador. Uma exclusão de arquivos infectados pode, na pior das hipóteses fazer com que o seu Windows não mais funcione e que uma reinstalação seja necessária.

Clicando agora no botão **Executar ações** o softwareG Data procederá da forma definida com cada detecção de vírus.

O seu sistema terá sido verificado quanto à existência de vírus. No entanto, se você tiver utilizado uma configuração com a opção Registrar, é possível que o seu computador não esteja livre de vírus.

4 Ao fim da verificação de vírus, você terá a possibilidade de transmitir uma cópia dos arquivos infectados para nós, para que possamos melhorar a proteção antiVirus para todos os usuários com base nesses dados. Naturalmente os seus dados serão tratados sigilosamente e nenhuma informação pessoal será repassada ou utilizada.

O repasse desses dados é totalmente voluntário e, se desejar, poderá ignorar esse ponto ou desativá-lo de forma permanente.

Vírus detectado

Quando o software G Data encontrar um vírus ou um outro programa malicioso no seu computador, você tem as seguintes possibilidades de tratar o arquivo infectado.

- **Somente registrar**: Na visualização **Registros** a infecção é relacionada. No entanto, não é feita a reparação ou exclusão do arquivo afetado. Porém, através do registro de vírus detectados você pode verificar individualmente os vírus e os remover objetivamente. **Atenção: Quando um vírus for somente registrado ele permanece ativo e perigoso.**

- **Desinfectar (se não for possível: mover para a quarentena)**: Aqui, tenta-se remover o vírus de um arquivo infectado, se não for possível sem danificar o arquivo, esse é movido para a **Quarentena**. Leia para isso também o capítulo: **Como funciona a quarentena?**
- **Mover arquivo para a quarentena**: Os arquivos infectados são movidos diretamente para a **Quarentena**. Na quarentena, os arquivos são armazenados criptografados. Ou seja, o vírus não pode causar nenhum dano e o arquivo infectado continuará existente para eventuais tentativas de reparação. Leia para isso também o capítulo: **Como funciona a quarentena?**
- **Excluir arquivo infectado**: Esta função só deve ser utilizada quando nenhum dado importante existir no seu computador. Uma exclusão de arquivos infectados pode, na pior das hipóteses fazer com que o seu Windows não mais funcione e que uma reinstalação seja necessária.

> **Quarentena e caixas postais de e-mail**: Existem arquivos os quais não é recomendável enviar para a quarentena, p.ex., os arquivos compactados para as caixas postais de e-mail. Quando uma caixa postal de e-mail é enviada para a quarentena, o seu programa de e-mail não poderá mais acessá-la e possivelmente não funcionará mais. Você deve ter cuidado especialmente nos arquivos com a extensão **PST**, pois estes, em geral, contêm os dados de sua **caixa postal de e-mail do Outlook**.

Feedback sobre malwares

Os G Data Security Labs pesquisam constantemente procedimentos para G Data proteger os clientes contra malware. Quanto mais informações existirem, mais eficazes poderão ser os mecanismos de proteção desenvolvidos. No entanto, muitas informações estão contidas em sistemas já atacados ou infectados. Para poder incluir também esse tipo de informação na análise, fundou-se a Iniciativa de informações sobre malware G Data. Nesse âmbito, as informações relevantes a malware são enviadas aos Security Labs G Data. Com a sua participação você contribui para que todos os clientes G Data possam usar a internet com mais segurança.

> **Malware**: É um termo genérico para todos os arquivos, programas e códigos que são programados para infectar, espionar ou controlar um computador sem o conhecimento do usuário. Entre eles estão, por exemplo, vírus, vermes, vírus de rootkit, cavalos de troia, registradores de teclado e muito mais.

Que dados são coletados?

Em princípio, dois tipos de dados são transmitidos: 1. Você pode enviar voluntariamente arquivos de malware para G Data e 2. são detectados conteúdos prejudiciais em uma página da web. Quando você envia arquivos com malware para a Internet Ambulance, além do arquivo, são enviados o local da detecção, o nome original do arquivo e a data da criação. Na detecção de conteúdos maliciosos da Internet, são enviados os seguintes dados:

- Número da versão do produto G Data e do mecanismo utilizado,
- Idioma (local) do sistema operacional,
- URL cujo acesso foi bloqueado e a razão (malware, phishing etc.)
- Nome do malware

Essas informações não são adequadas para identificar usuários do PC. Elas não serão comparadas aos dados pessoais.

Como os dados levantados são utilizados?

No processamento e no armazenamento dos dados, consideram-se os requisitos da lei sobre a proteção de dados e a disponibilização de dados dos respectivos países. G Data trabalha com o maior cuidado para proteger os dados contra acesso não autorizado. A avaliação dos dados acontece nos G Data Security Labs e serve para o esclarecimento de questões de pesquisa na área da segurança TI. A meta mais importante é a pesquisa de riscos de segurança e o desenvolvimento de mecanismos de proteção. Aos exemplos de utilização, pertencem, por exemplo, a criação de listas de bloqueio, a avaliação estatística para publicação em artigos especializados ou o desenvolvimento de conjuntos de regras para a tecnologia de proteção. A participação é voluntária e a recusa não tem nenhum efeito negativo no funcionamento do produto. Com a sua participação na Iniciativa de informações sobre malware G Data, futuramente todos os clientes G Data poderão ser informados e protegidos ainda melhor sobre ameaças de computadores.

Mensagem not-a-virus (não vírus)

Arquivos informados como **not-a-virus**, são aplicativos potencialmente perigosos. Tais programas, não dispõem diretamente de funções maliciosas, mas, no entanto, podem ser utilizados para ataques contra você. Estão incluídos nessa categoria, por exemplo, programas de serviço para administração remota, programas para comutação automática das teclas de função, clientes IRC, servidor de FTP ou programas distintos de serviço para criação ou para ocultar processos.

Quarentena

Durante a verificação de vírus você tem a possibilidade de proceder de diferentes maneiras com as **Detecções de vírus**. Uma opção é mover o arquivo infectado para a quarentena. A quarentena é uma área protegida dentro dentro do software onde os arquivos infectados são armazenados de forma codificada e, dessa forma, o vírus não pode mais ser repassado a outros arquivos.

Os arquivos em quarentena permanecem então no estado em que foram encontrados pelo softwareG Data e você pode decidir como deseja proceder.

- **Atualizar**: Se a caixa de diálogo para a quarentena tiver sido mantida aberta por um longo tempo e um vírus for encontrado e movido para a quarentena, nesse meio tempo, (por exemplo, automaticamente através da sentinela de vírus), a exibição poderá ser atualizada com esse botão.
- **Enviar**: Em determinados casos, você pode enviar um arquivo infectado que não pôde ser desinfectado para a G Data pela Internet. Naturalmente o conteúdo desse arquivo será tratado confidencialmente. O resultado dessa verificação flui para a melhoria e atualização das assinaturas de vírus e do software. Leia para isso também o capítulo: **Feedback sobre malwares**
- **Desinfectar**: Em muitos casos os arquivos infectados podem ainda ser salvos. O software remove então a parte virótica de um arquivo infectado e reconstrói assim, o arquivo original não infectado. Quando uma desinfecção é bem-sucedida, o arquivo é movido automaticamente para o local onde estava armazenado antes da verificação de vírus, e estará novamente disponível sem restrições.

- **Mover de volta**: Às vezes pode ser necessário mover de volta um arquivo infectado que não pôde ser desinfectado da quarentena para seu local de origem. Isso pode ser feito para salvar os dados. Essa função só deve ser utilizada em casos raros e sob rígidas condições de segurança (por ex., desconectar o computador da rede/Internet, fazer o backup antes de dados não infectados etc.).
- **Excluir**: Quando não precisar mais do arquivo infectado, você pode simplesmente exclui-lo da quarentena.

Registros

Na área de registros são listados os registros criados pelo software. Ao clicar no título das colunas **Hora de início**, **Tipo**, **Título** ou **Status**, você pode organizar respectivamente os registros existentes. Com os botões **Salvar como** e **Imprimir** dados de registro podem ser salvos como arquivos de texto ou serem impressos diretamente. Para excluir um registro, selecione o registro na tabela com o mouse e clique na tecla **Del** ou pressione o botão **Excluir**.

Licença múlti-usuário

Com uma licença multiusuário, você pode utilizar o software G Data na quantidade licenciada de computadores. Após a instalação no primeiro computador e da Atualização na Internet, você obterá os Dados de acesso transmitidos on-line. Quando você instalar seu software no próximo computador, você deve simplesmente informar o nome do usuário e a senha que você recebeu no registro no G Dataservidor de atualização. Repita o procedimento em cada instalação.

Utilize em todos os seus PCS os seus **Dados de acesso** (Nome de usuário e Senha) para a atualização na Internet, os quais foram fornecidos após o seu registro. Para isso, proceda como descrito a seguir:

1. Inicie o software G Data.

2. Na SecurityCenter, clique em **Assinaturas de vírus > Atualizar assinaturas de vírus**

3. Insira na janela exibida, os dados de acesso recebidos anteriormente por e-mail . Se clicar agora em OK o seu computador será licenciado.

Prorrogação da licença

Alguns dias antes de sua licença expirar, aparece uma janela de informações na barra de tarefas. Clicando, abre-se uma caixa de diálogo na qual você pode prorrogar a sua licença sem problemas diretamente, em poucos passos. Clique simplesmente no botão **Comprar agora**, complete os seus dados e a proteção antiVirus está novamente garantida imediatamente. A fatura será enviada nos próximos dias pelo correio.

Esta caixa de diálogo aparece apenas ao término de um ano. Depois disso, a sua licença G Data é prorrogada automaticamente a cada ano. Mas você pode cancelar essa assinatura a qualquer hora e sem mencionar as razões.

Troca de computador

Você pode utilizar o seu produto G Data em um novo ou em outro computador com os seus dados de acesso existentes. Instale simplesmente o software e informe os seus dados de acesso. Nesse caso, o servidor de atualização configura a conexão para o novo computador. Caso o software G Data ainda se encontre no antigo computador, é preciso transferir a licença deste para o novo. A quantidade de transferências de licenças é limitada - alcançado o valor limite, a licença é bloqueada completamente e não é mais possível carregar nenhuma atualização.

Desinstalação

Quando desejar remover em algum momento o software G Data do seu computador, a forma mais fácil de fazê-lo é, no G Data**Grupo de programas** , clicar no botão **Desinstalar**. A desinstalação ocorrerá de forma totalmente automática. Como alternativa, é possível executar a desinstalação no painel de controle do Windows.

- **Windows Vista**, **Windows 7**: Na barra de tarefas do Windows, clique no ícone Iniciar (normalmente na parte inferior à esquerda da sua tela) e selecione a pasta **Painel de controle**. Lá você encontrará o item **Programas > Desinstalar programas**. Selecione aqui o software G Data na lista e clique no botão **Desinstalar** para executar a desinstalação.

- **Windows XP**: Clique na barra de tarefas do Windows em **Iniciar** e selecione a pasta **Configurações > Painel de controle > Software**. Lá você encontrará, na guia **Instalar/Desinstalar**, a possibilidade de selecionar o software G Data com o mouse. Clique em seguida no botão **Adicionar/Remover** para executar a desinstalação.

Se durante a desinstalação ainda houverem arquivos na **Quarentena**do software G Data, será perguntado se esses arquivos deverão ser excluídos ou não. Se não excluir os arquivos, eles permanecerão em uma pasta G Dataespecial codificada em seu computador e, dessa forma, não poderão causar danos. Esses arquivos estarão novamente disponíveis quando o software G Data for reinstalado no seu computador. Durante a desinstalação será perguntado se você deseja excluir as **configurações e registros**. Se não excluir esses arquivos, os registros e as configurações estarão novamente disponíveis em uma reinstalação. Conclua a desinstalação clicando no botão Concluir. O software terá sido totalmente desinstalado do seu sistema.

Praga de computador

O **BootScan** ajuda a combater vírus que se aninharam em seu computador antes da instalação do software antivírus e que, possivelmente, podem impedir a instalação do G Data software. Para isso, existe uma versão especial do programa do software que pode ser executada já antes da inicialização do Windows.

O que significa um processo de inicialização? Quando você liga o seu computador, normalmente, o sistema operacional Windows é iniciado automaticamente. Este processo se chama **Dar um boot**. Existe também a possibilidade de iniciar outros programas automaticamente, ao invés do sistema operacional Windows. Para verificar a existência de vírus no seu computador antes da inicialização do Windows, a G Data disponibiliza, adicionalmente à versão do Windows, uma versão especial com capacidade de boot.

Como eu cancelo um BootScan? Se, após uma reinicialização, o seu computador não mostrar o habitual ambiente do Windows, mas uma interface especial do software G Data, isso não deverá ser motivo para preocupações. Se não tiver planejado nenhum BootScan, basta selecionar com as teclas de seta o registro **Microsoft Windows** e clicar em **Voltar**. O Windows inicializará normalmente, sem o BootScan.

Se desejar executar um **BootScan**, proceda da seguinte forma:

1a **BootScan com o CD do programa**: Utilize o CD do programa da G Data e faça com ele o boot no seu computador. - Insira o CD da G Data na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

1b **Faça o BootScan com o software G Data descarregado da Internet**: Através do registro Criar CD de boot da **G Data** no grupo de programas da **G Data** (*ícone do Windows na barra de tarefas > Todos os programas > Software G Data > Criar CD de boot*), você grava um novo BootCD.

Insira o seu próprio BootCD gravado na unidade. Na janela de inicialização aberta, clique em **Cancelar** e desligue o seu computador.

Se você usa o **Windows XP**, pode acontecer que, na tentativa de criar um BootCD, receba uma mensagem que o **IMAPI 2.x** não está instalado. Trata-se de uma atualização do Microsoft para sistemas operacionais antigos que é necessária para gravar mídias de dados. Você pode descarregar a atualização necessária diretamente da página inicial da Microsoft e instalá-la.

1c **Você tem uma versão especial para netbook do software G Data em um pen drive?** Aqui é possível executar o BootScan diretamente através do pen drive. No entanto, para isto, o seu netbook terá que ser capaz de dar o boot a partir de um pen drive.

Conecte o **G Data pen drive** com o seu netbook. Na janela de inicialização aberta, clique em **Cancelar** e desligue o Netbook.

Após a primeira etapa o BootScan para as três variações tem o mesmo procedimento:

2 Reinicialize o computador. O menu de inicialização do G Data **BootScan** aparece.

3 Com as setas, selecione a opção G Data**BootCD** e confirme a seleção com **Enter**. Um sistema operacional Linux será iniciado pelo CD e aparecerá uma versão especial da G Data para BootScans.

Se tiver problemas com a visualização da interface do programa, reinicialize o seu computador e selecione a opção G Data **BootCD – Alternativo**.

4 O programa irá sugerir agora a atualização das assinaturas de vírus.

Se você utiliza uma versão do software G Data que é compatível com as funções de backup, aqui você tem a possibilidade adicional de iniciar diretamente a reprodução de backups de seus dados armazenados.

5 Clique agora em **Sim**. Para poder executar a atualização, você deve inserir seus dados de acesso já recebidos ou seu número de registro. Depois disso, você pode executar a atualização. Assim que os dados tiverem sido atualizados na Internet, aparecerá o aviso **Atualização concluída**. Saia agora da tela de atualização clicando no botão **Fechar**.

A **atualização automática na Internet** é disponibilizada quando for utilizado um **roteador** que atribua endereços IP automaticamente (**DHCP**). Se não for possível a atualização na Internet, o **BootScan** poderá ser executado também com as assinaturas de vírus antigas. No entanto, nesse caso, após a instalação do software G Data , você deverá executar o mais rápido possível um novo BootScan com dados atualizados.

6 Agora você verá a interface do programa. Clique no registro **Verificar computador** e o seu computador será agora verificado quanto à existência de vírus e softwares maliciosos. Este processo pode levar uma hora ou mais, dependendo do tipo de computador e tamanho do disco rígido.

7 Se o software G Data encontrar vírus, remova-os com a ajuda da opção sugerida no programa. Após a remoção bem-sucedida do vírus, o arquivo original ficará novamente disponível.

8 Após concluir a verificação de vírus, saia do sistema clicando no x (no canto superior direito da janela).

9 Remova o CD do software G Data da unidade assim que a sua unidade for aberta ou desconecte o pen drive G Data do seu netbook.

10 Desligue novamente o seu computador e o reinicie. Agora, o seu computador inicializará novamente com o sistema operacional Windows padrão e você terá a garantia de poder instalar o software normal da G Data em um sistema sem vírus.

O que faço quando meu computador não faz o boot a partir do CD-ROM?

Se não for possível o boot a partir do CD/DVD-ROM, pode ser que essa opção precise primeiro ser ativada. Isto é feito na chamada **BIOS**, um sistema, que é inicializado automaticamente antes do sistema operacional Windows. Para fazer alterações na BIOS, execute as seguintes etapas:

1. Desligue o seu computador.
2. Reinicialize o computador. Normalmente, você consegue acesso à configuração da BIOS, ao iniciar (= Boot) o computador você pressionar a tecla **Del** (algumas vezes também a tecla **F2** ou **F10**).
3. A forma de alteração individual na configuração da BIOS é diferente de computador para computador. Leia para isto, a documentação do seu computador. Em resumo, a sequência do boot deve ser **CD/DVD-ROM:, C:** ou seja, a unidade de CD/DVD-ROM será o **1st Boot Device** e a partição do disco rígido, com o seu sistema operacional Windows, será o **2nd Boot Device**.
4. Salve as alterações e reinicie o seu computador. Agora o computador estará pronto para um BootScan.

O que faço quando o meu netbook (ou também PC desktop/ notebook) não faz o boot a partir do pen drive?

Se o seu computador não fizer o boot automaticamente a partir do pen drive, execute as seguintes etapas:

1. Desligue o seu computador.
2. Insira o G Data **pen drive** em uma **porta USB** livre do seu computador.
3. Ligue o seu computador.
4. Durante a inicialização, pressione a tecla **F2**, para chegar na **BIOS** do computador.
5. A interface da BIOS será exibida com uma barra de menu, onde você pode selecionar o menu **Boot** com as teclas de seta (para direita/esquerda). Agora, pressione **Enter**.
6. Você terá, então, a possibilidade de selecionar o registro **Hard disc drives** através das teclas de seta (para cima/baixo). Agora, pressione **Enter**.
7. Selecione agora o registro **USB** de forma que **1st Drive = USB** apareça em primeiro lugar (teclas **Enter** e de setas).

8. Pressione **F10**, para salvar e fechar a BIOS. O seu computador poderá agora fazer o boot a partir do pen drive.
9. Reinicialize o computador. Agora o computador estará pronto para um BootScan.

Dicas de comportamento

Apesar de o software G Data não detectar e remover apenas vírus conhecidos, mas, com a ajuda da análise heurística, reconhecer programas maliciosos desconhecidos até hoje, é sem dúvida melhor evitar logo de vez uma infecção por vírus. Para isso, algumas medidas de segurança devem ser atendidas, que não exigem muito esforço e que, no entanto, aumentam a segurança do seu sistema e dados consideravelmente.

- **Utilizar contas do usuário**: No seu computador você deve utilizar duas contas de usuário. Uma **conta de administrador**, que você sempre utiliza quando instalar softwares ou configurações básicas no seu computador e uma **conta de usuário** com direitos restritos. A conta de usuário, não deverá p.ex., poder instalar programas ou realizar modificações no sistema operacional do Windows. Com essa conta, você poderá então navegar relativamente seguro na Internet, pegar dados de computadores de terceiros e etc. A documentação da ajuda do sistema operacional Windows explica como criar diferentes contas de usuário.
- **Ignorar e-mails spam**: Cartas corrente e e-mails spam não devem ser respondidos por via de regra. Mesmo que esses e-mails não contenham vírus, eles sobrecarregam significativamente o fluxo de dados na Internet através de seu encaminhamento indesejado.
- **Verificar suspeita de vírus**: Se tiver uma suspeita de vírus fundamentada, p.ex., porque um novo software instalado não faz o que era esperado ou uma mensagem de erro aparecer, verifique o respectivo programa preferencialmente antes da reinicialização do computador, quanto à infecção de vírus. Isso é recomendável porque alguns cavalos de tróia executam os comandos de exclusão somente após a reinicialização do computador e, dessa forma, podem ser mais facilmente detectados e combatidos.
- **Windows Updates regulares**: Deve se tornar rotina a instalação dos atuais patches da Microsoft, porque esses fecham freqüentemente novas falhas de segurança detectadas do Windows, antes que um programador de vírus pense em utilizá-las para novas rotinas maliciosas. O Windows-Update também pode ser automatizado.

- **Utilizar software original**: Mesmo quando em raros casos a mídia de dados do software original esteja contaminada por vírus, a probabilidade de uma infecção por vírus através de cópias pirata ou cópias em mídias de dados regraváveis é significativamente maior. Por esse motivo, utilize apenas software original.
- **Tratar software da Internet com cuidado**: Ao fazer download de softwares da Internet, seja extremamente crítico e utilize apenas softwares realmente necessários cuja origem lhe pareça confiável. Nunca abra arquivos enviados por e-mail por desconhecidos ou que chegam de forma supreendente de amigos, colegas ou conhecidos. Verifique antes, através de uma consulta ao local correspondente, se o respectivo aplicativo pode ser iniciado sem perigo ou não.

Índice

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z